



# *Info@starklawlibrary.org*

*Stark County Law Library Association*

*May 2005*

## BEGINNERS

## Secretary of State Tips

**The email address, info@starklawlibrary.org really works! TRY IT!!**

LeapLaw <<http://www.leaplaw.com/>> is basically a pay-to-play site. You can pay \$15.00 for each successful search of the knowledge base, or you can pay \$125/month - \$1250 annually for anytime service. However, a large portion of their site is free, including an interesting use of a blog called the Secretary of State Tips. One possible reason that it is free to all could be that it is being underwritten by sponsors who provide corporate/UCC services - just the type of services in which someone using this site might be interested. <sup>1</sup>

Secretary of State Tips <<http://www.leaplaw.com/blawg/pub/pubhome.cfm?tid=1>> is really 50 blogs in one with an RSS feed for all 50 states, and one for each individual state. Each state link contains information about SOS activities and information. <sup>2</sup> and begins with the Basics Box containing information on Fax File, E File, Expedited Services, (for both UCC and Corporate entities) Name Reservations and Preclearance. Then follows the blog, which is very unusually listed in alphabetical order rather than reverse chronological.

The listings for Ohio and our surrounding states showed a great deal of currentness. The blog appears to have begun in February. Many of the entries had been updated and there were items as new as last week!

Each state's blog has some material in common:

- Contact Information for the Secretary Of State
- An Annual Report
- Where to File Foreign Corporation Amendments
- Foreign Qualification, Incorporated, Limited Partnership, and LLC Formation Summaries

If they can keep these blogs current, it will prove to be a very worthwhile asset.

Even in this age of rapid technology, corporate practitioners still have to make phone calls to paralegals or service companies asking "Can we fax file in [you name the state]?" "Can we get this merger document precleared?" etc. <sup>3</sup>

No More!

## INTERMEDIATE

## Acrobat Tag

**How do you think your clients would respond if they knew your "dirty little secret?"**

I haven't decided if this is a good thing or a bad thing, but I HAVE decided that it is worth your attention. Recently a company called Remote Approach, <<http://www.remoteapproach.com/>> has utilized an unexpected feature of Acrobat 7 which allows the use of a "tagging mechanism" [read web bug] to deliver a service that "helps companies and individuals who publish and distribute Adobe® Acrobat (PDF) documents to understand the reach and use of their materials." <sup>4</sup> When a reader opens a PDF document using Acrobat Reader 7, the Reader connects to <<http://www.remoteapproach.com/remoteproach/logging.asp>>. The information is submitted over port 80 using HTTP, making it unlikely that a normally configured home or office firewall would block the activity. <sup>5</sup>

Yes, it would be interesting to see who is reading our papers and how long they spend on them, and you aren't asking for any REALLY private data about the reader, but how comfortable would you be knowing that you were utilizing a web bug to gather this information? And how do you think your clients would respond if they knew your "dirty little secret?"

If you are using Adobe Acrobat Reader Version 7, here are some methods for not being tracked by the tagging mechanisms utilized by Remote Approach:

- Turning off JavaScript disables the document's code and prevents the "tagged" document from "phoning home." <sup>6</sup> The negative side to this solution is that it would also disable the "forms" and calculation features of version 7 and you may get a persistent popup dialog box asking you to turn Java back on.
- As long as Remote Approach continues to use just the one domain name, you could set your firewall to block all transmissions to that site.
- Use an older version of Acrobat Reader.
- Or use one of the many free alternatives to Adobe.
  1. GNOME Ghostview PDF viewer. This utility seems to lack a web site, though there is an online manual <<http://www.gnome.org/~shaunm/doctable/docs/ggv/HEAD/index.html>> available which is only slightly out of date.
  2. The KDE contribution in the PDF viewer arena is kghostview <<http://docs.kde.org/en/3.3/kdegraphics/kghostview>>.
  3. Xpdf is a non-ghostscript reader from <<http://www.foolabs.com/xpdf/>>.
  4. Gpdf <<http://www.inf.tu-dresden.de/~mk793652/gpdf/>> is a GNOME-based PDF viewer built upon xpdf. <sup>7</sup>

## ADVANCE

## "Phish in Your IM"



and



Phishing and viruses are two of the problems that have moved from the realm of e-mail into the field of Instant Messaging. Since we have not actually dealt with this topic yet, I have consulted the Wikipedia for a definition:

In computing, **phishing** is the act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by masquerading in an official-looking email, IM, etc. as someone trustworthy with a real need for such information. It is a form of social engineering attack.

Typically, a phishing email will appear to come from a trustworthy company and contain a subject and message intended to alarm the recipient into taking action. A common approach is to tell the recipient that their account has been deactivated due to a problem and inform them that they must take action to re-activate their account. The user is provided with a convenient link in the same email that takes the email recipient to a fake webpage appearing to be that of a trustworthy company. Once at

that page, the user enters her personal information which is then captured by the fraudster.<sup>8</sup>

Recently, I have come across a pair of particularly timely blog entries on security issues and IM. One by Tom Mighell at Inter Alia:

Those dastardly phisherpeople aren't just attacking us through e-mail... I'd think we'd all know better than to assume the friends on our IM lists are going to be asking us for our User IDs and passwords. But just in case..... don't ever respond to such an IM! If you really want to know, send a separate IM to your friend, or call them on the phone, to verify whether he or she really wants your password. I'm sure she doesn't.<sup>9</sup>

And the other is from Genie Tyburski at TVC Alert:

"Reuters had to shut down instant messaging access after a new worm infiltrated and infected the system. The worm generated fake messages that lured people to a Web site that further distributed the attack."<sup>10</sup> Her blog references "Worm Attack Forces Reuters IM Offline" at <[http://news.com.com/Worm+attack+forces+Reuters+IM+offline/2100-7355\\_3-5671139.html](http://news.com.com/Worm+attack+forces+Reuters+IM+offline/2100-7355_3-5671139.html)>.

## FOOTNOTES

- <sup>1</sup> Truman, R. "Secretary of State Tips: 50 States in One Blog." 25 March 2005. Paul L. Boley Law Library. 14 April 2005. <<http://lawlib.lclark.edu/boleyblogs/index.php?p=670>>.
- <sup>2</sup> Mighell, Tom. "Blawg of the Day." 24 March 2005. Inter Alia. 13 April 2005. <[http://www.inter-alia.net/comments.php?id=P2592\\_0\\_1\\_0](http://www.inter-alia.net/comments.php?id=P2592_0_1_0)>.
- <sup>3</sup> Svenson, Ernest and Dave Fishel. "Corporate Law Information." 8 March 2005. PDF for Lawyers. 14 April 2005. <[http://www.pdfforallawyers.com/2005/03/corporate\\_law\\_i.html](http://www.pdfforallawyers.com/2005/03/corporate_law_i.html)>.
- <sup>4</sup> Pacifici, Sabrina I. "Site Reports That Web Bugs Can Be Activated With Adobe 7." beSpacific. 7 April 2005. BeSpacific LLC. 15 April 2005. <<http://www.bespacific.com/mt/archives/007932.html#7932>>.
- <sup>5 & 6</sup> "Unexpected Features in Acrobat 7." LWN.net. 30 March 2005. Eklektix, Inc. 18 April 2005. <<http://lwn.net/Articles/129729/>>.
- <sup>7</sup> "The Grumpy Editor's Guide to PDF Viewers." LWN.net. November 2004. Eklektix, Inc. 18 April 2005. <<http://lwn.net/Articles/113094/>>.
- <sup>8</sup> "Phishing." Wikipedia: The Free Encyclopedia. 19 April 2005. <<http://en.wikipedia.org/wiki/Phishing>>.
- <sup>9</sup> Mighell, Tom. "Phish in your IM." 8 April 2005 Inter Alia. 18 April 2005 <[http://www.inter-alia.net/comments.php?id=P2638\\_0\\_1\\_0](http://www.inter-alia.net/comments.php?id=P2638_0_1_0)>.
- <sup>10</sup> Tyburski, Genie. "Reuters' IM Goes Offline." TVC Alert. 15 April 2005. Ballard Spahr Andrews & Ingersoll, LLP. 18 April 2005. <<http://www.virtualchase.com/tvcalert/apr05/15apr05.html#im>>.

By Nancy Stinson, MLS  
nancy@starklawlibrary.org